REMARKS

In view of the following remarks, Applicants respectfully request reconsideration of the present application.

Objections and Rejections

The Office Action dated January 14, 2004:

1. objects to the specification;
2. rejects claims 1, 3, 4, 7, 8, 10, 12, 13, 16 and 17 under 35 U.S.C. § 103(a) for obviousness based upon:
   a. the Lewis patent; in view of
   b. the Sibigtroth, et al. patent;
3. rejects claims 6 and 15 under 35 U.S.C. § 103(a) for obviousness based upon:
   a. a combination of the Lewis and Sibigtroth, et al. patents; in view of
   b. United States Patent no. 5,313,639 entitled "Computer With Security Device for Controlling Access Thereto" which issued May 17, 1994, on a patent application filed by George Chao ("the Chao patent"); and
4. rejects claims 2, 5, 9, 11, 14 and 18 under 35 U.S.C. § 103(a) for obviousness based upon:

a. a combination of the Lewis and Sibigtroth, et al. patents; in view of

b. United States Patent no. 5,594,319 entitled "Battery Pack Having Theft Deterrent Circuit" that issued January 14, 1997, on a patent filed by Iilonga P. Thandiwe ("the Thandiwe patent").

The Claimed Invention

The invention, as presently encompassed by independent claim 1, is an integrated circuit pre-boot security controller that includes a non-volatile password memory for storing at least one user password. A password input circuit, included in the pre-boot security controller, receives a password for comparison with any user passwords recorded in the password memory. If the pre-boot security controller is in a security operating mode, a digital logic circuit, also included in the pre-boot security controller, compares the received password with any user passwords recorded in the password memory. If the password received by the password input circuit matches a user password recorded in the password memory, an output circuit of the pre-boot security controller, that is coupled to the digital logic circuit, transmits an output signal to a power subsystem to enable energizing operation of a digital computer.

The Cited References

The Lewis patent

The Lewis patent beginning in col. 6 at line 59 declares that:

> **[a] thief** who removes a device protected by the present invention **will be unable to use the device**, and thus once aware that the device is so protected will likely be deterred from removing it. Emphasis supplied.

A description of the structure and operation of the Lewis patent's invention, which allegedly achieves the result described in the preceding quotation therefrom, appears in an October 17, 2003, Response to a prior Office Action dated July 16, 2003. Applicants hereby incorporate by reference the description of the Lewis patent's invention that appears in the prior October 17, 2003, Response.

As set forth both in the prior October 17, 2003, Response, and in the accompanying "Declaration of Brian Oh," by using an in-circuit emulator (ICE):[1]

1. the Lewis patent's predetermined primary security code, i.e. predetermined primary password, can be easily obtained; and

---

[1] For example, see United States Patent No. 4,900,014 ("the '014 patent") that issued May 4, 1999, for a more complete description of how an ICE may be used to acquire data that is being accessed by a microprocessor. Copies of the Abstract and FIG. 2 of the '014 patent attached as Exhibit A to the October 17, 2003, Response are hereby incorporated by reference.

2. therefore, the invention disclosed in that reference truly provides only an illusion of security.

In view of the purpose for the invention disclosed in the Lewis patent which appears in the excerpt therefrom set forth above, Applicants respectfully submit that **the invention disclosed in the Lewis patent**, since it truly provides only an illusion of security, **is** therefore:

1. **inoperable for its intended purpose** as stated in the excerpt which appears above from the Lewis patent; and
2. **the Lewis patent does not truly enable its alleged invention**.

The Sibigtroth, et al. patent

The Sibigtroth, et al. patent discloses a "data processor with memory within a single integrated circuit package provides a programmable 'secure mode' of operation to selectively restrict access and protect information stored in its memory." (Abstract)

The data processing system 10 includes a single integrated circuit package portion 11 and a peripheral portion 12 having an external peripheral device. (Col. 2, lines 19-22) The integrated circuit package portion 11 includes:

1. a memory 13;
2. a data processor 14;

3. a decoder 16;

4. an instruction inhibit circuit 18; and

5. a programmable security device 20. (Col. 2, lines 22-25)

Attached as Exhibit A to the accompanying "Declaration of Brian Oh," is a copy of FIG. 1 of the Sibigtroth, et al. patent that has been annotated with a dashed line to encloses the integrated circuit package portion 11 of the data processing system 10. (Col. 2, lines 26-49) The integrated circuit has memory with programmable security from unauthorized observation of internal processing operations in response to receipt of externally provided signals. (Col. 1, line 49-53)

The integrated circuit package portion 11 operates in three different modes:

1. a "single chip mode;"

2. an "expanded mode;" and

3. a "secure mode." (Abstract)

When the integrated circuit package portion 11 operates in the "single chip mode," the data processor 14 accesses both data and instructions strictly from within the integrated circuit package portion 11. (Abstract) "The single chip mode of operation requires data processor 14 to address predetermined memory locations of memory 13 via address bus 22 for the purpose of either reading instructions and data from memory 13 or writing data to

memory 13." (Col. 3, lines 3-8) "The single chip mode is characterized by the fact that only memory 13 and data processor 14, along with address bus 22 and data/instruction bus 24 are utilized." (Col. 3, lines 12-14)

When the integrated circuit package portion 11 operates in the "expanded mode," the data processor 14 may access either the internal memory 13 or external memory for both instructions and data. (Abstract)

> In the expanded mode of operation, data processor 14 can access either memory 13 or peripheral portion 12 for both instructions and data. Expanded mode operation utilizes memory 13, data processor 14, address bus 22, data/instruction bus 24, data/instruction bus 30 and instruction inhibit circuit 18. Since expanded mode operation allows data processor 14 to read instructions from peripheral portion 12, **the instructions presented to data processor 14 via data/instruction buses 24 or 30, may be readily observed or interrupted for the purpose of reading or modifying the contents of memory 13; therefore the expanded mode of operation is not secure**. (Col. 3, lines 19-31) (Emphasis supplied.)

The secure mode of operation restricts accesses of instructions to memory contained within the single integrated circuit while allowing data accesses to memory either internal or external to the integrated circuit." (Abstract)

> "The secure mode of operation is a mix between the single chip and the expanded modes of operation. In the secure mode of operation, instruction read cycles performed by the data processor are confined to the data processor as in the single chip mode, whereas **data reads and writes initiated by the data processor can be made either internal or external to the data processor in an expanded mode of operation**. **The secure mode of operation**

> **provided herein is an effective and economical solution to isolate instruction information of a data processor while allowing the data processor to read or write non-proprietary data external to the data processor.**
>
> * * *
>
> However, regardless of the variety of operations considered permissible within a single chip or expanded mode of operation, the functionality of the secure mode insures that memory 13 may not be read or modified by unauthorized sources external to the single integrated circuit package. (Col. 4, lines 34-60) (Emphasis supplied.)

The Chao patent

The Chao patent beginning in col. 1 at line 38 states that:

> an objective of the present invention is to provide a computer with **a push-button control device** which is adapted to be received in a disk drive receiving space of the computer and **which can prevent the operation of the computer in the absence of a correct input password.**
>
> Another objective of the present invention is to provide a computer with a push-button control device which locks the computer keyboard and disables the floppy disk drive and the main system board of the computer in the absence of a correct input password.

A description of the structure and operation of the Chao patent's invention appears in an October 17, 2003, Response to a prior Office Action dated July 16, 2003. Applicants hereby incorporate by reference the description of the Lewis patent's invention that appears in the prior October 17, 2003, Response.

The Thandiwe patent

The Thandiwe patent beginning in col. 1 at line 47 states that:

> there exists a need in a smart battery pack for a **theft deterrent circuit**, and particularly one which disables the battery pack from unauthorized use. (Emphasis supplied.)

A description of the structure and operation of the Thandiwe patent's invention appears in an October 17, 2003, Response to a prior Office Action dated July 16, 2003. Applicants hereby incorporate by reference the description of the Lewis patent's invention that appears in the prior October 17, 2003, Response.

Argument

Objection to the Specification

The Office Action dated January 14, 2004, objects to line 21 on page 15 of the application as originally filed because it contains an embedded hyperlink and/or other form of browser-executable code.

Applicants respectfully submit that the October 17, 2003, Response, beginning on page 7 and continuing onto page 9, amends the text of the specification on page 15 in line 21 as originally filed to eliminate the embedded hyperlink and/or other form of browser-executable code. Therefore, the Applicants respectfully:

1. submit that the text of the specification as amended by the October 17, 2003, Response traverses the objection thereto that appears in the Office Action dated January 14, 2004; and

2. request that the objection thereto which appears in the Office Action dated January 14, 2004, be immediately withdrawn.

The Pending Claims Traverse
Rejection for Obviousness

In rejecting claims 1, 3, 4, 7, 8, 10, 12, 13, 16 and 17 under 35 U.S.C. § 103(a) for obviousness, the January 14, 2004, Office Action combines the Sibigtroth, et al. patent with only the Lewis patent stating:

> Sibitroth (sic) discloses a controller and memory as part of an integrated circuit (Sibitroth [sic] Col 2 lines 19-25). It would be obvious to one skilled in the art to construct the microcomputer of Lewis in the method of Sibitroth [sic] because it is more compact.

The accompanying "Declaration of Brian Oh" in paragraph nos. 16 and 24 establishes that:

> if an in-circuit emulator ("ICE"), such as that disclosed in United States Patent No. 5,900,014 entitled "External Means of Overriding and Controlling Cacheability Attribute of Selected CPU Accesses to Monitor Instruction and Data Streams" ("the '014 patent") that issued May 4, 1999, were coupled to the microcomputer 10 disclosed in the Lewis patent, the ICE could be used to read out the "predetermined primary security code stored in PROM 34."

> The Lewis patent clearly discloses that the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, i.e. predetermined primary password, stored in PROM 34.

The facts established by paragraph no. 16 quoted above from the "Declaration of Brian Oh" establishes that, contrary to the assertion which begins in col. 6 at line 59 of the Lewis patent:

1. a thief who removes, i.e. steals, a device protected by the invention disclosed in that reference will be able to easily use the device after recovering the predetermined password from the PROM 34 using an ICE; and
2. therefore, inclusion of the invention disclosed in the Lewis patent in a device will not deter someone from removing, i.e. stealing, the device.

For the preceding reasons, the invention disclosed in the Lewis patent:

1. truly provides only an illusion of security; and
2. does not enable the invention alleged in that reference because the invention does not prevent use of a stolen device.

Regarding combining the disclosure of the Sibigtroth, et al. patent with that of the Lewis patent, the accompanying "Declaration of Brian Oh" in paragraph nos. 32-34 first establishes that:

> [i]f constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as

> suggested at the bottom of page 4 in the January 14, 2004, Office Action retains the PROM 34 for storing the predetermined primary security code, i.e. predetermined primary password, then **the predetermined primary password may be easily obtained using an ICE as the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with the predetermined primary security code, i.e. predetermined primary password, stored in PROM 34**. (Col. 3, lines 50-53)
>
> Therefore, **constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action does not alter the security provided by the invention disclosed in the Lewis patent if the predetermined primary security code, i.e. predetermined primary password, is stored in the PROM 34 external to the Sibigtroth-style microcomputer 10**.
>
> If constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action retains the PROM 34 for storing the predetermined primary security code, i.e. predetermined primary password, then **it will be no more compact than the disclosure of the Lewis patent**.

Regarding combining the disclosure of the Sibigtroth, et al. patent with that of the Lewis patent, the accompanying "Declaration of Brian Oh" in paragraph nos. 35 and 37-41 further establishes that:

> constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action **is more compact and betters the security provided by the Lewis patent only if the predetermined primary security code, i.e. predetermined primary password, were stored in the memory 13 of the integrated circuit package portion 11**.
>
> Referring again to Exhibit A, it is also readily apparent that even when the integrated circuit package portion 11 operates either in its "secure mode" or in its "single chip" mode, an ICE connected to the integrated circuit package portion 11 can monitor and record, via

the address bus 22 which extends from inside the integrated circuit package portion 11 outside to the peripheral portion 12, all addresses from which the data processor 14 fetches data and instructions from the memory 13.

Since col. 3, lines 50-53 of the Lewis patent discloses that the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, if a Sibigtroth-style microcomputer 10 stored the Lewis patent's predetermined primary security code, i.e. predetermined primary password, in its memory 13, and if the Sibigtroth-style microcomputer 10 were operating in its "secure mode," by monitoring the address bus 22 an ICE connected to the integrated circuit package portion 11 can record all addresses in the memory 13 from which the data processor 14 fetches data and instructions while comparing keystroke by keystroke the keyed in security code, i.e. password, with the predetermined primary security code, i.e. predetermined primary password stored in the memory 13.

Using an ICE, having thus monitored and recorded all addresses in the memory 13 from which the data processor 14 fetches data and instructions while comparing keystroke by keystroke the keyed in security code, i.e. password, with the predetermined primary security code, i.e. predetermined primary password, one could then readily ascertain the predetermined primary security code, i.e. predetermined primary password, by operating the integrated circuit package portion 11 in its "expanded mode" and exporting from the integrated circuit package portion 11 to the ICE the data stored in the memory 13 at the address previously monitored and recorded using the ICE.

Thus, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action merely makes ascertaining the predetermined primary security code, i.e. predetermined primary password, a two step operation, i.e. first record the addresses in the memory 13 and then obtain from the memory 13 the data stored at those addresses, rather than a one step operation.

Finally, regarding the disclosure of the Sibigtroth, et al. patent, the accompanying "Declaration of Brian Oh" in paragraph nos. 42 and 43 observes that:

> constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action and storing the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11 fails to provide non-volatile password storage.
>
> Consequently, if one were to construct the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action and were to store the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11, due to a lack of non-volatile storage the predetermined primary security code, i.e. predetermined primary password, would be forever lost if electrical power were removed from the integrated circuit package portion 11.

Summarizing facts established by the accompanying "Declaration of Brian Oh:"

1. there exist two (2) possible ways for constructing the Lewis patent's microcomputer 10 in the method of the integrated circuit package portion 11 disclosed in the Sibigtroth, et al. patent, i.e.:
   a. one which retains the Lewis patent's PROM 34 and stores the password in the PROM 34 external to the integrated circuit package portion 11; and
   b. one which omits the Lewis patent's PROM 34 and stores the password in the memory 13 of the

Sibigtroth, et al. patent's integrated circuit package portion 11;

2. retaining the Lewis patent's PROM 34 for storing the predetermined password external to the integrated circuit package portion 11:

   a. does not increase the illusory security provided by the Lewis patent since the predetermined password may still be easily obtained using an ICE; and

   b. is no more compact;

3. omitting the Lewis patent's PROM 34 and storing the predetermined password in the memory 13 of the Sibigtroth, et al. patent's integrated circuit package portion 11:

   a. still permits ascertaining the predetermined password in a two step operation using an ICE, i.e.:

      i. first recording with an ICE the addresses in the memory 13 while entering a password; and

      ii. then exporting from the memory 13 with the ICE the data stored at those addresses while the integrated circuit package portion 11 operates in its expanded mode; and

   b. if the predetermined password were stored in the memory 13 of the integrated circuit package portion

11 which lacks non-volatile storage, the predetermined password would be forever lost if electrical power were removed from the integrated circuit package portion 11.

Thus, facts established by the accompanying "Declaration of Brian Oh" prove that combining the disclosure of the Sibigtroth, et al. patent with that of the Lewis patent:

1. does not increase the illusion of security provided by the invention disclosed in the Lewis patent; and
2. in the second way of combining the disclosures, produces a combination which:
   a. does not meet all the limitations expressly set forth in independent claim 1 because it lacks a "non-volatile password memory;" and
   b. is inoperable for the intended purpose expressly set forth in the Lewis patent.

For the preceding reasons, claims 1, 3, 4, 7, 8, 10, 12, 13, 16 and 17 traverse rejection under 35 U.S.C. § 103(a) for obviousness based upon:

c. the Lewis patent; in view of
d. the Sibigtroth, et al. patent.

Furthermore, because independent claims 1 and 10 traverse rejection under 35 U.S.C. § 103(a), Applicants respectfully submit that

claims 2, 5, 6, 9, 11, 14, 15 and 18, which respectively depend either directly or indirectly from independent claim 1 or 10, also traverse the rejections set forth in the January 14, 2004, Office Action.

Conclusion

First, Applicants respectfully submit that the specification as amended in the October 17, 2003, Response traverses the objection thereto in the January 14, 2004, Office Action.

Second, Applicants respectfully submit that pending claims 1-18 all traverse rejection for obviousness under 35 U.S.C. § 103(a) on the bases set forth in the January 14, 2004, Office Action because combining the disclosure of the Sibigtroth, et al. patent with that of the Lewis patent:

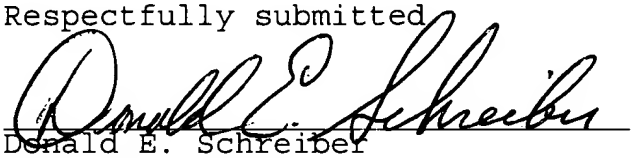
1. does not increase the illusion of security provided by the invention disclosed in the Lewis patent or enable the invention alleged in the Lewis patent because that invention, even i the microcomputer 10 disclosed in the Lewis patent were constructed in the method of the Sibigtroth, et al. patent, does not prevent use of a stolen device; and
2. in one way of combining the disclosures, produces a combination which:

a. does not meet all the limitations expressly set forth in independent claim 1; and

b. is inoperable for the intended purpose expressly set forth in the Lewis patent.

Since the Applicants in the October 17, 2003, Response committed to furnishing formal drawings when there are allowed claims, Applicants respectfully request that all objections and rejections appearing in the January 14, 2004, Office Action be withdrawn, and that this patent application pass immediately to issue.

Respectfully submitted,



Donald E. Schreiber
Reg. No. 29,435

Dated: 1 March, 2004

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicants